VDA Support of BCA Demonstration

John Pawling

jsp@jgvandyke.com

J.G. Van Dyke & Associates, Inc;

a Wang Government Services Company

VDA Bridge CA (BCA) Support

- **Enhance Certificate Management Library (CML).**
- **Enhance S/MIME Freeware Library (SFL).**
- **Provide facilities support, installation, integration and hosting of BCA demonstration(s) (hardware not included).**

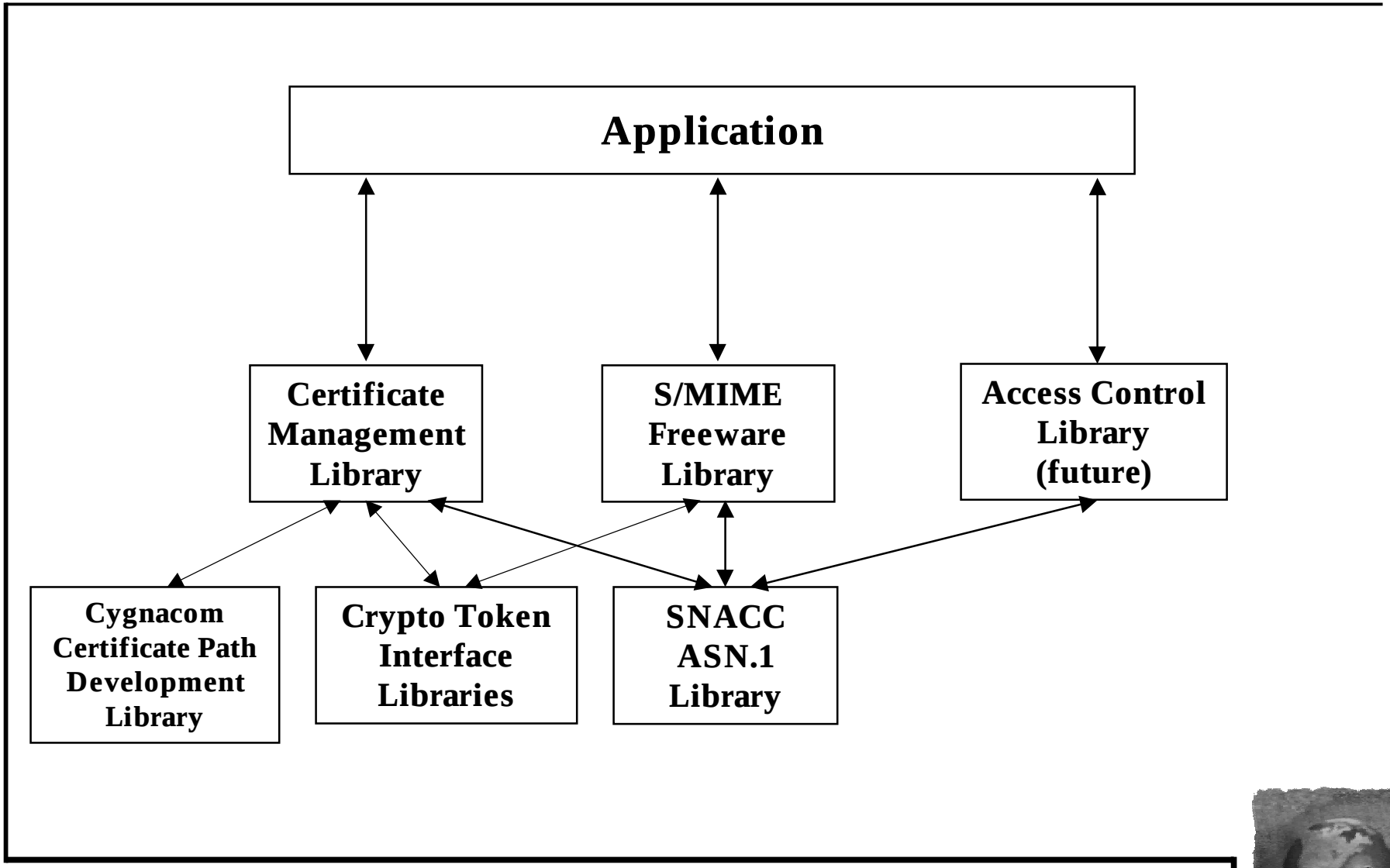
VDA/V32 Security Services Objectives

- **Provide freeware reference implementations of:**
  - **X.509 version 3 certification path verification**
  - **Rule Based Access Control**
  - **IETF S/MIME version 3**
  - **Abstract Syntax Notation One (ASN.1) encoding/decoding**
- **Provide unencumbered source code for libraries**
- **Provide modular, high-level, platform-independent interface:**
  - **Allows application developers to meet security requirements with minimal effort**
  - **Allows developers to use only the libraries required for their particular application**

Security Services Modular Architecture

- **Certificate Management Library (now available)**
  - **Validates X.509 certification paths and CRLs**
  - **Provides local cert/CRL storage functions**
  - **Provides LDAP v2**
- **S/MIME Freeware Library (now available)**
  - **Implements IETF S/MIME v3 security heading**
  - **Includes security label, signed receipts, mail list options**
- **Access Control Library (available in 2000)**
  - **Provides Rule Based Access Control using security labels and certificate authorizations (SDN.801)**
  - **msp4_acdf now available, implements SDN.801**

Security Services Modular Architecture



S/MIME Freeware Library

- **SFL is a freeware implementation of IETF S/MIME v3 RFC 2630 (Cryptographic Message Syntax) & RFC 2634 (Enhanced Security Services) specifications.**
- **When used with Crypto++ library, SFL implements RFC 2631 (Diffie Hellman).**
- **SFL supports the use of RFC 2632 (Certificate Handling) and RFC 2633 (Message Spec).**
- **Goal: To provide a reference implementation of RFC 2630 and RFC 2634 to encourage their acceptance as Internet Standards.**

S/MIME Freeware Library

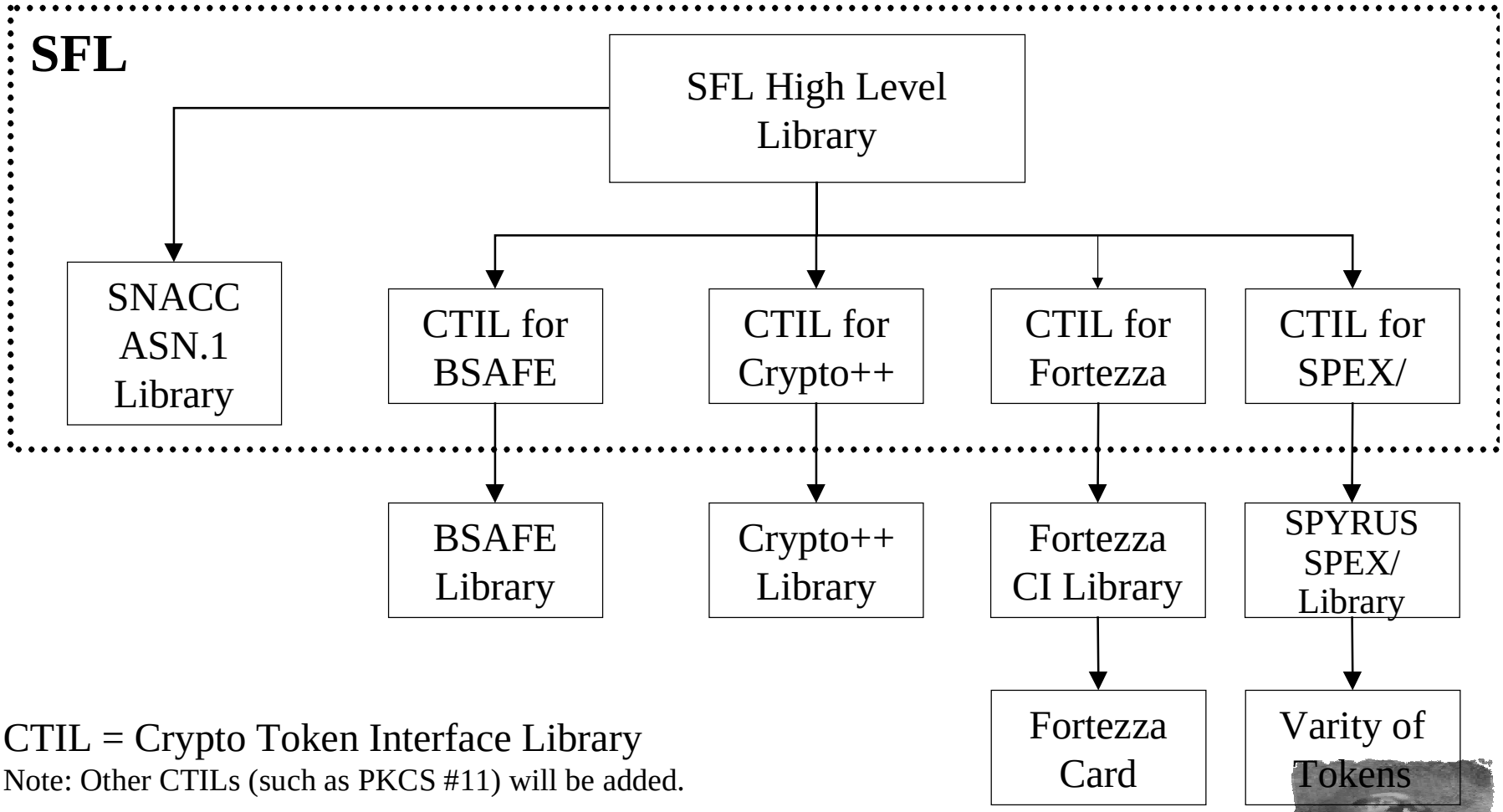
- **Protects any type of data (not just MIME).**
- **Algorithm independent: SFL is used with external crypto libraries that provide the crypto algorithms.**
- **Uses VDA-enhanced SNACC freeware library to perform all ASN.1 encoding (including DER) and decoding of CMS and ESS objects as well as certificates, CRLs, etc.**
- **All SFL source code is provided.**
- **SFL does not build/process MIME headings.**

S/MIME Freeware Library

Implements optional RFC 2634 security services:

- **Signed receipts – provides authenticated proof of delivery (similar to registered mail).**
- **Security labels – provides the capability to label data with sensitivity values (i.e., company proprietary).**
- **Mail list information – provides the capability to allow mail lists to expand secure messages.**
- **Signing Certificate attribute - identifies signer's certificate(s) and certificate policies.**

SFL Architecture



CTIL = Crypto Token Interface Library

Note: Other CTILs (such as PKCS #11) will be added.

SFL Components

- **SFL High Level library**
  - **Builds and processes CMS and ESS objects independent of the crypto library in use**
  - **Provides full C++ API and limited C API**
- **SNACC ASN.1 library (VDA enhanced)**
  - **Implements ASN.1 Distinguished Encoding Rules**
- **Crypto Token Interface Libraries (CTIL)**
  - **Isolates the SFL High Level classes from the specifics of the cryptographic token processing**
  - **Calls the cryptographic token functions to perform the Encrypt, Decrypt, Sign, Verify operations**

Crypto Token Interface Libraries (CTILs)

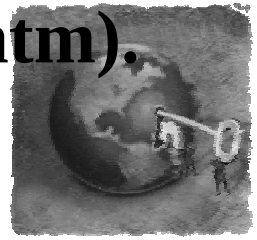
- **BSAFE CTIL**
  - **Calls RSA BSAFE library providing RSA algorithms (RSA, RC2, MD5) for backwards compatibility.**
- **Crypto++ CTIL**
  - **Calls Crypto++ library providing mandatory S/MIME v3 algorithms (3DES, E-S D-H, SHA-1, DSA).**
- **Fortezza CTIL**
  - **Calls U.S. Government's Fortezza Cryptologic Interface library providing SKIPJACK, Key Exchange Algorithm, SHA-1 and DSA**
- **SPEX/ CTIL**
  - **Calls Spyrus SPEX/ library providing access to a variety of crypto tokens/algorithms. Still testing.**

SFL Interoperability Testing

- **SFL used to exchange signedData and envelopedData messages with MS Internet Explorer Outlook Express v4.01 and Netscape Communicator 4.X. Signed messages have been exchanged with RSA S/MAIL, WorldTalk and Entrust S/MIME v2 products.**
- **S/MIME v3 interop testing between SFL and MS includes all envelopedData features such as using E-S D-H pairwise key with 3DES-wrapped and RC2-wrapped CEKs. RSA-signed signedData messages have also been exchanged. Majority of ESS features tested. Still need to finish signed receipt testing.**
- **Also tested with Baltimore and Entrust.**

SFL Availability

- **Organizations can use the SFL as part of their applications without paying any royalties or licensing fees (see SFL Public License).**
- **VDA-enhanced SNACC ASN.1 software and SFL documents are freely available to everyone at: http://www.jgvandyke.com/services/infosec/sfl.htm**
- **All other portions of the SFL are available at: http://www.armadillo.huntsville.al.us/software/smime and are export controlled as per U.S. Government Export Administration Regulations (http://www.bxa.doc.gov/Encryption/Default.htm).**



Certificate Management Library

- **X.509 Certification Path Validation**
  - **supports both v3 X.509 certs and Fortezza v1 certs**
- **ASN.1 Decoding**
- **Local Certificate/CRL Storage**
- **Directory Retrieval via LDAP v2**
- **Uses Cygnacom Certificate Path Development Library (CPDL) to robustly build cert paths**
- **Meets all BCA requirements (tested with SPYRUS SPEX/ library and Lynks Card)**

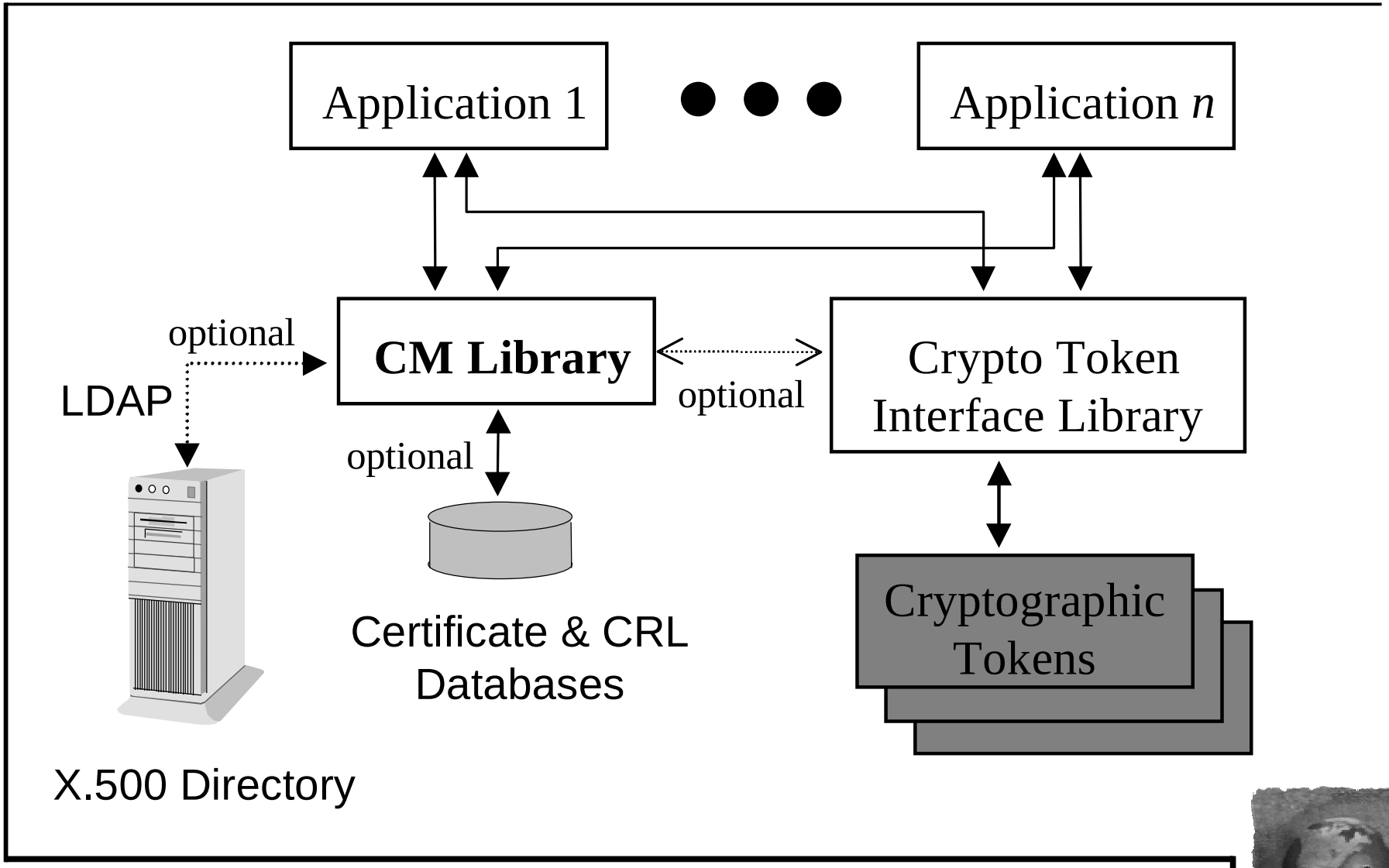
CML X.509 Compliance

- **Implements all 1997 X.509 features (except Delta CRLs) and cert path validation requirements such as:**
  - **name chaining (including multi-valued RDNs)**
  - **key identifier chaining**
  - **signature verification (using DSA and RSA)**
  - **validity date checking**
  - **revocation checking**
  - **name constraints**
  - **basic constraints**
  - **certificate policies, mappings and constraints**
  - **subject and issuer alternate names**
  - **key usage/extended key usage**
  - **private key usage period**
  - **CRL distribution points (VDA has license from Entrust)**
  - **cross certificates (when used with Cygnacom CPDL)**
  - **CRL extensions and CRL entry extensions**

CML Compliance

- **Compliant with SDN.706 except that commPrivileges/ SigOrKMPrivileges subordination and CRL number checks are not performed. (CML uses the proper CRL based on thisUpdate rather than CRL number.)**
- **CML complies with majority of PKIX requirements in RFC 2459. PKIX requirements the CML doesn't support: Delta CRLs; use of name constraints other than DNs; use of UTF8String in DNs; use of empty subject DNs; processing of PKIX extended key usage OIDs; and processing of Authority Information Access extension. Note that the CML correctly returns errors if any unsupported extensions are marked critical.**

CML Interactions



J.G. Van Dyke & Associates, Inc.
People Making Information Technology Work Securely

CML API Overview

- **Session Management**
  - **CML uses session ID to support multiple applications.**
- **Certificate Operations**
  - **Retrieve, decode, validate CRLs and certs**
- **Database Management**
  - **Add, delete, list, retrieve from local database**
- **Memory Management**
  - **Functions to free memory allocated by the CML**

Certificate Validation Steps

- **Application sets *initial-policy-set* and *initial-explicit-policy-indicator* and *initial-inhibit-policy-mapping-indicator* values by calling CM_SetPolicy().**
- **Application validates a certificate by calling CM_RetrieveKey().**
- **If errors occur, application can check the specific X.509 errors by calling CM_GetErrInfo().**

CML Availability

- **Organizations can use the CML as part of their applications without paying any royalties or licensing fees (see CML Public License).**
- **CML was originally developed by V32. VDA is enhancing/supporting CML under contract to V32.**
- **Uses VDA-enhanced SNACC freeware library to ASN.1 encode/decode certs, CRLs, etc.**
- **All CML source code is provided.**
- **CML is available at: http://www.armadillo.huntsville.al.us/software.**

VDA Point of Contact

John Pawling, jsp@jgvandyke.com

J.G. Van Dyke & Associates, Inc.,

a Wang Government Services Company

141 National Business Pkwy, Suite 210

Annapolis Junction, MD 20701

(301) 939-2739 or (410) 880-6095